REMARKS

Claims 1-7, 9-19, 21-31, and 33-43 are all the claims pending in the application. By this Amendment, Applicant editorially amends claim 25 to broaden the scope of the invention. The amendment to claim 25 does not narrow the literal scope of the claims and thus does not implicate an estoppel in the application of the doctrine of equivalents. The amendment to claim 25 was not made for reasons of patentability. Moreover, Applicant amends claim 37 to further clarify the invention.

Claim Rejections under 35 U.S.C. § 112

The Examiner rejected claim 29 under section 112, second paragraph for improper antecedent basis. Independently, Applicant has amended claim 25 to broaden the scope of the claim. This coincidentally overcame all of the Examiner's problems with claim 29. Therefore, Applicant respectfully requests the Examiner to withdraw this rejection of claim 29.

Claim Rejections under 35 U.S.C. § 103

Applicant thanks the Examiner for withdrawing the previous rejection. The Examiner, however, found new grounds for rejecting the claims. Claims 1-7, 9-19, 21-31, and 33-43 are rejected under 35 U.S.C. § 103(a).

In particular, claims 1-7, 9-11, 13-19, 21-23, 25-31, 33-35, and 41-43 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings Cryptograph and Network Security 2nd Edition (hereinafter "Stallings") in view of Bryant "Designing an Authentication System: a Dialogue in Four Scenes" (hereinafter "Bryant"), and further in view of two newly found

references, Applied Cryptography by Schneier (hereinafter "Schneier") and U.S. Patent No. 5, 953, 504 to Sokal et al. (hereinafter "Sokal"). Claims 12, 24, and 36 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Bryant, Schneier, Sokal, and further in view of U.S. Patent No. 6,463,474 to Fuh et al (hereinafter "Fuh"). Claims 37-40 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Bryant, Schneier, Sokal, Fuh and further in view of Method of Communicating Application to VeriSign (hereinafter "VeriSign"). Applicant respectfully traverses these rejections in view of the following comments.

Stallings, Bryant, Schneier, and Sokal

The Examiner rejected claims 1-7, 9-11, 13-19, 21-23, 25-31, 33-35, and 41-43 under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Bryant, and further in view of two newly found references, Schneier and Sokal.

Of the rejected claims, only claims 1, 13, 25, and 43 are independent. This response will initially focus on these independent claims. Among a number of unique features of claim 1, not taught or suggested by the prior art, is "...generating an authentication key based on a user name and a computer identifier...wherein said authentication key includes a server user identifier." The Examiner asserts that claim 1 is directed to a user authentication method and is obvious over Stalling, Bryant, Schneier, and Sokal. Applicant respectfully disagrees.

Applicant respectfully submits that one of ordinary skill in the art would not have been motivated to combine the four references in a manner alleged by the Examiner and that the Examiner is exercising impermissible hindsight in attempting to combine these four references.

In addition, Applicant respectfully submits that even if the four references are somehow combined, they fail to teach or suggest all the limitations of the independent claim 1.

The initial burden of establishing that a claimed invention is *prima facie* obvious rests on the USPTO. *In re Rijckaert*, 9 F.3d 1531, 1532 (Fed. Cir. 1993), MPEP § 2143.01. To make its *prima facie* case of obviousness, the USPTO must satisfy three requirements:

a) The prior art relied upon, coupled with the knowledge generally available in the art at the time of the invention, must contain ***some suggestion or incentive*** that would have motivated an artisan to modify a reference or to combine references. *In re Thrif*, 298 F.3d 1357, 1363 (Fed. Cir. 2002).

b) The proposed modification of the prior art must have had a reasonable expectation of success, and that determined from the vantage point of the artisan at the time the invention was made. *Amgen, Inc. v. Chugai Pharm. Co.*, 927 F.2d 1200, 1209 (Fed. Cir. 1991).

c) The prior art reference or combination of references must teach or suggest all the limitations of the claims. *In re Vaeck*, 20 U.S.P.Q.2d 1438, 1442 (Fed. Cir. 1991); *In re Wilson*, 424 F.2d 1382, 1385 (CCPA 1970).

The motivation, suggestion or teaching may come explicitly from statements in the prior art, the knowledge of one of ordinary skill in the art, or, the nature of a problem to be solved. *In re Dembiczak*, 175 F.3d 994, 999 (Fed. Cir. 1999). Alternatively, the motivation may be implicit from the prior art as a whole, rather than expressly stated. *Id.* Regardless if the USPTO relies on an express or an implicit showing of motivation, ***the USPTO is obligated to provide particular***

findings related to its conclusion, and those findings must be clear and particular. *Id.* ***A broad conclusionary statement, standing alone without support, is not "evidence."*** *Id.; see also, In re Zurko*, 258 F.3d 1379, 1386 (Fed. Cir. 2001).

In addition, ***a rejection cannot be predicated on the mere identification of individual components of claimed limitations.*** *In re Kotzab*, 217 F.3d 1365, 1371 (Fed. Cir. 2000). Rather, particular findings must be made as to the reason the skilled artisan, ***with no knowledge of the claimed invention***, would have selected these components for combination in the manner claimed. *Id.*

A critical step in analyzing the patentability of claims pursuant to section 103(a) is casting the mind back to the time of invention, to consider the thinking of one of ordinary skill in the art, guided only by the prior art references and the then-accepted wisdom in the field. *See In re Kotzab*, 55 USPQ2d 1313, 1316 (Fed. Cir. 2000) (*citing In re Dembiczak*, 175 F.3d 994, 999, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999)). ***Close adherence to this methodology is especially important in cases where the very ease with which the invention can be understood may prompt one " to fall victim to the insidious effect of a hindsight syndrome wherein that which only the invention taught is used against its teacher."*** *Kotzab,* 55 USPQ2d at 1316 (*quoting W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1553, 220 USPQ 303, 313 (Fed. Cir. 1983)).

Hindsight has repeatedly been held to be improper and ineffective in supporting an argument of *prima facie* obviousness. *See, e.g., In re Fritch*, 23 USPQ2d 1780 (Fed. Cir. 1992); *In re Bond*, 15 USPQ2d 1556 (Fed. Cir. 1990); *In re Laskowski* 10 USPQ2d 1397 (Fed. Cir.

1989). On the present record, the references simply do not provide the impetus to do what the inventor did.

The Examiner alleges that one of ordinary skill in the art would have been motivated to combine Stallings and Bryant to prevent identity duplicity by ascertaining a user by a unique name and a computer identifier (see page 5 of the Office Action). In addition, the Examiner alleges that one of ordinary skill in the art would have been motivated to combine Stallings, Bryant, Schneier, and Sokal to "enable secrets to be secured and accessed only by authorized users and for the user to use the secret to obtain the services of a server" (see page 6 of the Office Action).

Applicant respectfully points out that Bryant is a printed publication and as such should be enabling. Bryant, however is only a dialogue suggesting theoretical design for the authentication system. Bryant does not teach or suggest the actual implementation of a system, which would include the network addresses. In short, Bryant is not an enabling printed publication.

Moreover, Schneier is very different from Stallings and Bryant. Stallings and Bryant address the problem of access control by a variety of users. In other words, Stallings and Bryant are related to providing a user with a key to access a protected, secure system.

Schneier, on the other hand, is related to splitting a secret (a message) amongst a number of users to prevent each individual user to gain access without the other (page 70). That is, Schneier teaches not allowing an individual user to access a protected item alone. In Schneier, each user must combine his or her part of a message, for example, to access the protected item.

The Examiner alleges that Schneier teaches "the user to use the secret to obtain the services of a server." Schneier, however, teaches just the opposite. Schneier teaches that a user will not be able to access a service and that only a number of users combined (by combining their part of the secret) can access the service, *e.g.*, Trent splits a secret between Alice and Bob, or Alice, Bob, Carol, and Dave (pages 70 to 73).

One of ordinary skill in the art would not have combined Schneier with Stallings and Bryant at least because that would mean that the users would have to get together to access a secret item, alleged service, as opposed to each user obtaining access to the service. In short, one of ordinary skill in the art would not have been motivated to combine the three references in the manner suggested by the Examiner. In addition, one of ordinary skill would not have turned to the secret sharing scheme when designing a Kerberos system so as to provide each user with his or her own individual access. The only reason to turn to Schneier is to try to meet the novel features of claim 1. But for the present invention, there is no reason to turn to the secret sharing scheme of Schneier.

Moreover, the Examiner alleges that one of ordinary skill in the art would further combine Stallings, Bryant, Schneier, and Sokal. Sokal relates to allowing public access to a secure terminal while allowing the user from the public to enter payment and to access the internet for a payment received from the user (col. 1, lines 44 to 50). Sokal teaches that a user can register by providing a name, address, a credit card number, and so on. In response to this information, the server will generate an ID code and a secret password which will be used

continually by the user to identify that user in the server and to obtain access (col. 5, lines 43 to 57).

In Sokal, the user must remember his user ID and password for each type of system. The server must manage all of these individual user IDs and their passwords. In other words, Sokal is no different from the prior art disclosed in the specification, in that it creates an administrative nightmare in managing individual user IDs and passwords for each service. Bryant clearly teaches away from such a system. In particular, in Bryant, Euripides criticizes the system of Sokal as being clumsy by requiring a password and ID for each service (page 3). Moreover, in Sokal, there are no tickets, authentication keys, or encryption. In fact, Sokal is not even related to how the connection is established, instead Sokal is more concerned with billing the user when the service is accessed from a public terminal. In other words, there is no motivation to combine user ID code and secret password of Sokal with Stallings, Bryant and/or Schneier.

Moreover, the Examiner alleges that Schneier's secret can be "an ID code" of Sokal (page 6 of the Office Action). Applicant respectfully disagrees. There is no motivation to split Id code and provide each user with only a portion of the ID code as it would mean that each user could not individually access the service. Moreover, the object of Sokal's system is to bill the user for the service. If users were to share an ID, the server would not know which user to bill. Indeed, one of ordinary skill in the art would not use an ID code of Sokal as a "secret" of Schneier. In short, Applicant respectfully submits that there is no motivation for combining the four references in the manner suggested by the Examiner. Accordingly, the Examiner cannot fulfill the motivation prong of a *prima facie* case of obviousness.

Moreover, Stallings, Bryant, Schneier, and Sokal, either alone or in combination, fail to teach or suggest a number of features of the independent claim 1. In the conventional unified logon systems, each client computer connected to a database server computer, needs to have a corresponding user identifier and password created on the server computer, in addition to having a user name and a password to log onto the client computer. This requirement creates an administrative nightmare because of maintaining and managing all the client user names and passwords with the corresponding server user IDs and passwords. Moreover, when a server password or ID is changed, the system administrator needs to notify the users of their new password or server ID, creating additional security risk of the message being intercepted by hackers. In the method as set forth in claim 1, however, the authentication key is generated "based on a user name and a computer identifier" and the authentication key "includes a server user identifier." As a result, the administrator need not forward the server ID to the user. Instead, the server ID is sent to the user in an authentication key based only on the user name and a computer identifier received from the user.

The Examiner appears to acknowledge that both Stallings and Bryant fail to teach or suggest having the user only sending the user name and a computer identifier and receiving a ticket with the server ID. The Examiner, however, alleges that the combined teachings of Schneier and Sokal teaches generating an authentication ticket with server ID based on a user name and a computer (see page 6 of the Office Action). The Examiner compares secret splitting to having an authentication key with a server ID. The teachings of Schneier, however, is not

related to an authentication key or a server ID. In Schenier, a secret is split amongst users, wheres an authentication key is for access to a service by an individual user.

Moreover, in Schneier, each user has a portion of a secret that the other user does not have. In other words, in Schneier secret sharing involves providing a portion of the secret only known to a first user without allowing the second user to know what is that portion of the secret that is only known to the first user. In Schneier, each entity only has a portion of a secret and never the whole secret. In other words, Schneier fails to teach or suggest providing an entity or a user with the entire secret. Schneier also fails to teach or suggest a server user identifier or an authentication key. In short, Schneier does not teach or suggest generating an authentication key based on a user name and a computer identifier, where the authentication key also includes a server user identifier.

The Examiner appears to acknowledge that Schneier does not teach or suggest a server user identifier. The Examiner, however, alleges that Sokal cures the deficient teachings of Schenier (page 6 of the Office Action). Sokal teaches that in response to a user registering its information (including a credit card number), the user is provided with an ID code and a secret password, which the user can use to access a service (col. 5, lines 54 to 63). In Sokal, there is no teaching of an authentication key or that an authentication key will include an ID code. Moreover, Sokal's ID code is created for each user to access a service. In other words, Sokal's method teaches that the server and the user will know the individual ID and password of this user. Sokal, however, fails to teach or suggest generating an authentication key, or generating a

key based on user name and a computer identifier, where the authenticiation key will include a server user identifier.

Therefore, "...generating an authentication key based on a user name and a computer identifier...wherein said authentication key includes a server user identifier," as set forth in claim 1 is not suggested or taught by the combined teachings of Stallings, Bryant, Schneier, and Sokal which lack having the user only send the user name and a computer identifier and the server creating an authentication key based on the user name and the computer identifier, where the authentication key will include the server user identifier. Together, the combined teachings of these references would not have (and could not have) led the artisan of ordinary skill to have achieved the subject mater of claim 1. Since claims 1-7 and 9-11 are dependent upon claim 1, they may be patentable at least by virtue of their dependency.

Next, Applicant respectfully traverses this rejection with respect to independent claims 13 and 25. These independent claims recite: "generating an authentication key that includes a server user name based on a user name and a computer identifier." This recitation is similar to the features argued above with respect to claim 1. Therefore, those arguments are respectfully submitted to apply with equal force here. For at least substantically the same reasons, therefore, Applicant respectfully requests the Examiner to withdraw this rejection of independent claims 13 and 25. Claims 14-19 and 21-23, and claims 26-31 and 33-35 are patentable at least by virtue of their dependency on claims 13 and 25, respectively.

Claims 41 and 42 are patentable at least by virtue of their dependency on claim 1. Moreover, claim 41 is patentable at least by virtue of its recitation of "the computer identifier

split into portions and the portions being interposed between the user name, the server user identifier and the server password prior to encryption." The Examiner alleges that the Initial Permuation of a DES scheme as taught by Schneier meets this exemplary feature of claim 41 (see page 9 of the Office Action). Applicant respectfully submits that Schneier only teaches shifting bits to various positions (pages 271-273). Schneier, however, fails to teach or suggest having portions of the computer identifier being interposed between user name, the server user identifier and the server password prior to encryption. In short, Schneier does not teach or suggest an encryption scheme set forth in claim 41. For at least this additional reason, Applicant respectfully submits that claim 41 is patentable over the combined teachings of Stallings, Bryant, Schneier, and Sokal.

Next, Applicant respectfully traverses this rejection with respect to independent claim 43. This independent claim recites: "generating an authentication key based on a user name and a computer identifier ... wherein said authentication key includes a user identifier for the computer connected to the data store." This recitation is similar to the features argued above with respect to claim 1. Therefore, those arguments are respectfully submitted to apply with equal force here. For at least substantically the same reasons, therefore, Applicant respectfully requests the Examiner to withdraw this rejection of independent claim 43.

Stallings, Bryant, Schneier, Sokal and Fuh

Claims 12, 24, and 36 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Bryant, Schneier, Sokal, and further in view of Fuh. Applicant respectfully traverses this rejection with respect to claims 12, 24, and 36, which depend on independent

claims 1, 13, and 25, respectively. Applicant has already demonstrated that the combined teachings of Stallings, Bryant, Schneier, and Sokal do not meet all the requirements of independent claims 1, 13, and 25. Fuh is relied upon only for its teaching of intercepting client request to access a server (see pages 10-11 of the Office Action). In short, Fuh does not compensate for the deficient teachings of Stallings, Bryant, Schneier, Sokal, and Fuh. Together, the combined teachings of these references would not have (and could not have) led the artisan of ordinary skill to have achieved the subject matter of independent claims 1, 13, and 25. Since claims 12, 24, and 36 are dependent upon claims 1, 13, and 25, respectively, therefore, they are patentable at least by virtue of their dependency.

Stallings, Bryant, Schneier, Sokal, and VeriSign

Claim 37 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Bryant, Schneier, Sokal, and VeriSign. Applicant respectfully traverses this rejection with respect to the dependent upon claim 1, claim 37. Applicant has already demonstrated that the combined teachings of Stallings, Bryant, Schneier, and Sokal do not meet all the requirements of independent claim 1. VeriSign is relied upon only for its teaching of emailing a certificate to a user (see pages 11-12 of the Office Action). In short, VeriSign does not compensate for the deficient teachings of Stallings, Bryant, Schneier, and Sokal. Together, the combined teachings of these references would not have (and could not have) led the artisan of ordinary skill to have achieved the subject matter of independent claim 1. Since claim 37 depends on claim 1, it may be patentable at least by virtue of its dependency.

In addition, claim 37 recites "wherein when the server user identifier changes, a new authentication key is generated and emailed to the user." The combined teachings of Stallings, Bryant, Schneier, Sokal, and Verisign fail to teach or suggest emailing a new authentication key when the server user identifier is changed. For at least this additional reason, claim 37 is patentable over the combined teachings of Stallings, Bryant, Schneier, Sokal, and Verisign.

Stallings, Bryant, Schneier, Sokal, Fuh, and VeriSign

Claims 38-40 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Bryant, Schneier, Sokal, Fuh, and further in view of Method of Communicating Application to VeriSign (hereinafter "VeriSign"). Applicant respectfully traverses this rejection with respect to the dependent upon claim 1, claims 38-40. Applicant has already demonstrated that the combined teachings of Stallings, Bryant, Schneier, Sokal, and Fuh do not meet all the requirements of independent claim 1. VeriSign is relied upon only for its teaching of emailing a certificate to a user (see pages 11-12 of the Office Action). In short, VeriSign does not compensate for the deficient teachings of Stallings, Bryant, Schneier, Sokal, and Fuh. Together, the combined teachings of these references would not have (and could not have) led the artisan of ordinary skill to have achieved the subject matter of independent claim 1. Since claims 38-40 depend on claim 1, they may be patentable at least by virtue of their dependency.

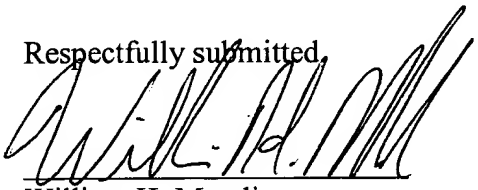
Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the

Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly invited to contact the undersigned attorney at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,



William H. Mandir
Registration No. 32,156

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: November 12, 2004